DETAILED ACTION

1. The request filed on September 08, 2008 for a request for continued examination (RCE) under 37 CFR 1.114 based on patent application 10/656,439 is acceptable and an RCE has been established. Claims 5, 14 and 23 are canceled. Thus **claims 1-4, 6-13, 15-22 and 24-30** are pending of which claims 1, 10 and 19 are independent claims.

2. Applicant's representatives Shun Yao Registration No. 59,242 and Examiner conducted a telephone interview on August 21, 2008. The subject matter of the interview is attached.

3. Both Applicant's representatives, and Examiner agreed on the claim language; in particular all parties discussed on how the claims should be amended to overcome the ground of rejection and possibly make the claims allowable. **Accordingly independent claims 1,10 and 19 are amended to incorporate the claim language discussed in the interview.**

Priority

4. This application claims priority of a provisional application 60/480,909 filed on June 24, 2003. Therefore, the effective filling data for the subject matter defined in the pending claims of this application is **06/24/2003.**

Allowable Subject Matter

5. **Claims 1-4, 6-13, 15-22 and 24-30** are allowed.

6. The following is an examiner's statement of reasons for allowance:

All independent claims **1, 10 and 19** are amended.

Before the independent claims were amended, the art on the record discloses the every limitation recited in the independent claims.

For instance, referring to the pervious independent claims 1 and 10 and 19, the art on the record, in particular, Hermann, the primary reference on the record, discloses a computer controlled method comprising:

- Establishing communication between a situation notification device [see , paragraph 0020, "first device"] and a provisioning device [see , paragraph 0020, "second device/servicing device"] over a preferred channel [See, paragraph 0020, "communication link"];[paragraph 0020, lines 15-21]

- Prior to establishing the communication, pre-authenticating the situation notification device to ensure that the situation notification device has physical access to the preferred channel. *[Paragraph 0021-0022] (On paragraph 0021, the following has been disclosed. "For establishing an authenticated session between the user's personal device and the serving device, e.g. a bank terminal, the user points with the personal device to the serving device or at least in this direction and passes via a unidirectional wireless communication channel, e.g. via an infrared channel, a sequence or an initial-sequence that comprises a password, a public key, a*

session key, identification parameters, and/or communication parameters. After receiving the sequence, the serving device responds by sending back over wireless broadcast medium encrypted information which can only be decrypted and used by the personal device. The respond may comprise information, a key, also a session key, and communication parameters from the serving device for further communication over the wireless broadcast medium. The personal device receives the encrypted information." Furthermore on paragraph 0022, the following has also been disclosed. "For a secure session over the wireless broadcast medium keys are exchanged. Thus, an encrypted communication over the wireless broadcast medium can take place." This implies the fact that prior to an encrypted communication between the situation notification device/first device/user's personal device and the servicing device the notification device/first device/user's personal device is pre-authenticated.)

- Providing provisioning information to said situation notification device over said preferred channel,[Paragraph 0020, lines 44-48] *(After receiving the sequence, the serving device responds by sending back over a wireless broadcast medium a respond. And as it is disclosed on paragraph 0020, lines 44-48 such responds may comprises, a key, also a session key and a*

communication parameters which meets the limitation of provisioning information from serving device to personal device/situation notification for further communication. In other words the personal device/situation notification device is provided with key, session key and a communication parameters/provisioning information)

wherein said situation notification device is automatically configured to receive subject matter information responsive to said provisioning information; *[Paragraph 0020, lines 48-49] (And the situation notification device is automatically configured to receive the encrypted information which meets the limitation of the subject matter information)*

- Receiving said subject matter information; [Paragraph 0020, lines 48-49] (encrypted information)

- Verifying said subject matter information with said provisioning information; [Paragraph 0014] *(Only the intended receiver/notification device receives the encrypted subject matter since it is the one that has the corresponding decryption key and the encrypted information/subject matter information with the corresponding private key/public key/session key/provisioning information are decrypted and*

verified that the subject matter is sent form the right provisioning device.)

- Presenting said subject matter information to a user of the situation notification device responsive to the step of verifying, wherein the step of verifying ensures that the subject matter information is genuine.. [Paragraph 0014 & abstract] *(Only the intended receiver/notification device receives the encrypted subject matter since it is the one that has the corresponding decryption key. And the encrypted information/subject matter information is presented to a user of the situation notification device only and only if the situation notification device carries the corresponding private key/public key/session key/provisioning information and successfully decrypts and verifies that the subject matter is sent form the right provisioning device, by doing so the situation notification device ensures that the subject matter information is genuine. This is simply another application of public key cryptograph, explained on paragraph 0014 and secure transmission disclosed in the abstract.)*

Hermann does not explicitly disclose the limitation recited as "wherein the preferred channel does not require being resistant to eavesdropping."

However, in the same field of endeavor Stirbu on paragraph 0008, discloses that a TLS Handshake Protocol allows a server and client in a communication session to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data. The TLS Handshake Protocol provides connection security having three basic properties: the peer's identity can be authenticated using asymmetric, or public key, cryptography (e.g., RSA, DSS, etc.); the negotiation of a shared secret is secure in that the negotiated secret is unavailable to eavesdroppers, and for any authenticated connection the secret cannot be obtained, even by an attacker who can place himself in the middle of the connection; and the negotiation is reliable in that no attacker can modify the negotiation communication without being detected by the parties to the communication.

However, as applicant's representative persuasively argued, after the present amendment, the combination of the art on the record does not disclose the specific functional limitation which is added to the respective independent claims.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submission should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am --4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

09/12/2008

/Samson B Lemma/
Examiner, Art Unit 2132

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132